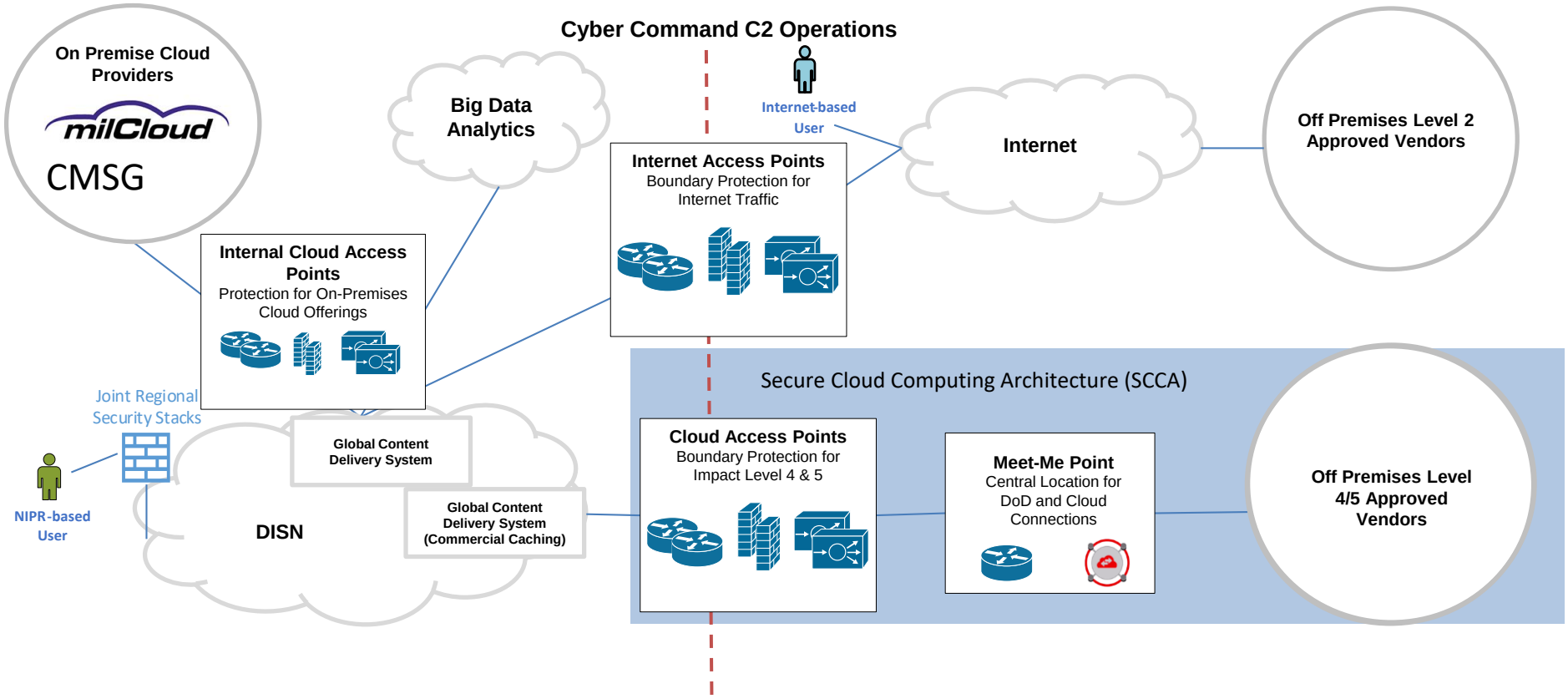
DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

# Secure Cloud Computing Architecture (SCCA)

## Program Overview

Bernard del Rosario
Chief Engineer, SCCA
May 14, 2019

# DoD Commercial Cloud Deployment Approach



# Overview

## Enterprise
SCCA provides a standardized approach to cloud access and security

## DoD Required
The portfolio includes mandated services to connect impact level 4/5 data to the commercial cloud

## Open Framework
SCCA security services connect to approved on and off premise cloud environments

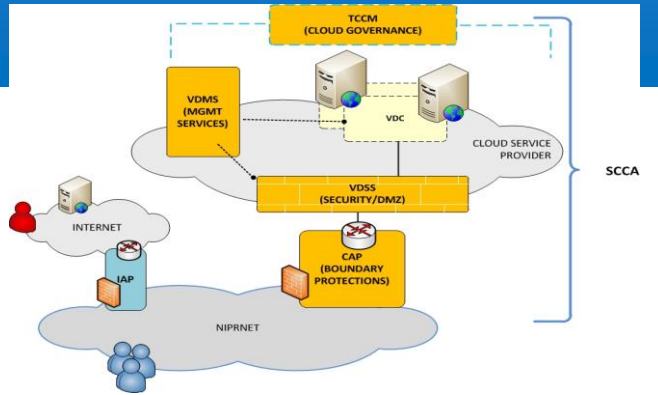
## Mission Tailored
Acquire services based on your mission requirements

## Performance Metrics
Real-time performance and security data

**Cloud Access Points (CAP):** Provides connectivity to approved cloud providers, and protects the DISN from cloud originated attacks

**Virtual Data Center Security Stack (VDSS):** Virtual Network Enclave Security to protect applications and data

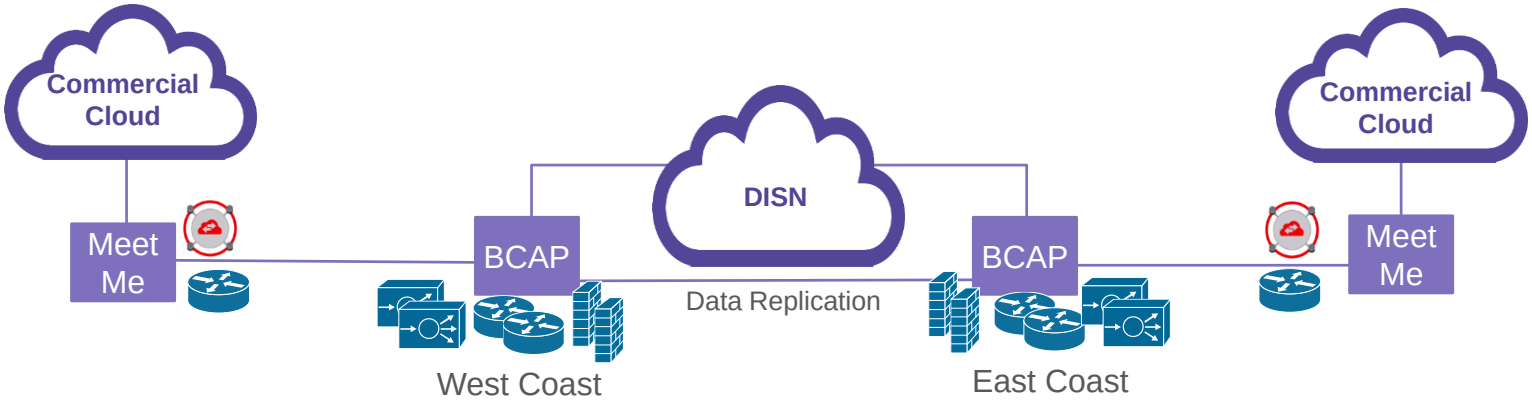
**Virtual Data Center Managed Services (VDMS):** Application host security, patching, configuration, and management



# Current Cloud Access Points Overview

## Boundary Cloud Access Points (BCAP)

- Two Locations: Camp Roberts, CA and the Pentagon
- 10G connections: local and geographical diversity
- Connects approved workloads to Level 4/5 Authorized Clouds



# Evolving Cloud Access, Security, and Management Services

## Previous State

### Previous Generation

- Two sites; 5G total
- Co-located with federated gateways
- Security managed by application owners
- Limited enterprise visibility and performance metrics

## Current State

### Second Generation

- Boundary CAP: two sites;10G
- Internal CAP: two sites; 10G
- Dedicated circuits
- Application security and management services
- Intelligence dashboard and cybersecurity service provider data feeds

## Future State

### Next Generation

- Boundary CAP: four sites;20G
- Internal CAP: two sites; 20G
- SIPR Boundary and internal: four sites; 20G
- CAP colocation at meet-me

# Services and Management Roles and Responsibilities

- Boundary defense: firewall and routers

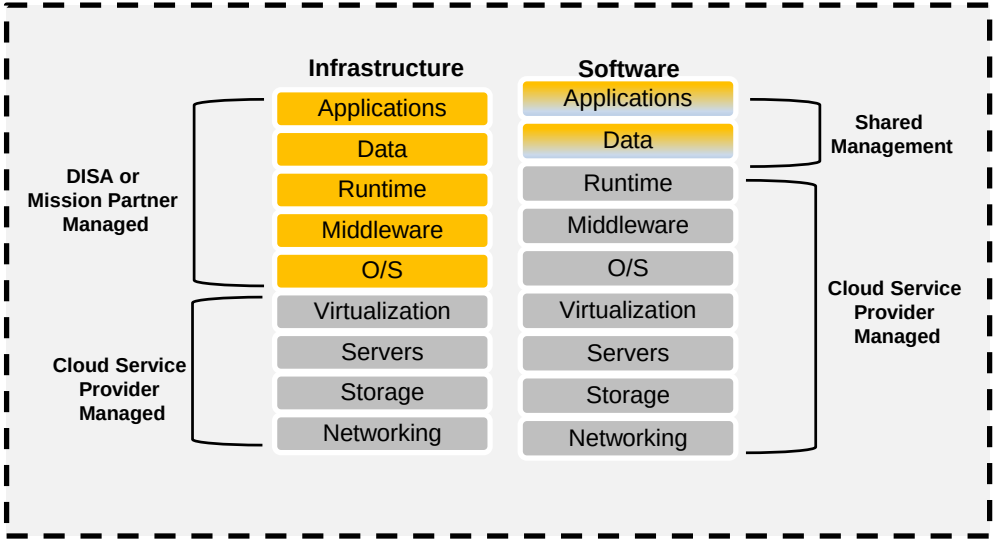
→ CAP

- Web application firewalls
- Next generation firewalls

→ VDSS

- Host based security services
- Assured Compliance Assessment Solution
- Operating system patching
- Recursive DNS Caching
- Cloud Visibility
- Privileged user access and password management

→ VDMS



# Features Overview

**Connect:** Access DoD approved level 4/5 cloud service providers.

**Secure:** Extend application and data-level security services to the cloud.

**Manage:** Obtain custom analytics and intelligence data for host based security and role based access controls.

**Boundary Defense:** Connect to approved Level 4/5 providers and protect DoD networks

**Web Application Firewalls:** Prevent targeted attacks; cross-site scripting, forceful browsing, cookie poisoning, and invalid input

**Next Generation Firewalls:** Virtual appliance architected to identify network traffic and implement policies in a mission-centric fashion

**Host Based Security Service:** Develop cloud-based orchestration for security policies, upgrades, and reporting

**Assured Compliance Assessment Solution:** Manage roles, scan zones, and policies

**System Patching:** Cloud-based DOD patch repositories

**Recursive Domain Name System Caching:** Forward and cache external queries

# Service Offerings

| Capability | BCAP | ICAP | VDSS | VDMS | TCCM |
|---|---|---|---|---|---|
| Boundary Defense | ✓ | ✓ | | | |
| Web application and next generation firewalls | | | ✓ | | |
| Host based security services | | | | ✓ | |
| Assured Compliance Assessment Solution | | | | ✓ | |
| Operating system patching | | | | ✓ | |
| Recursive Domain Name System Caching | | | | ✓ | |
| Cloud Visibility | | | | ✓ | |
| Privileged user access and password management | | | | | ✓ |

# Cloud Connection Process Summary

## Phase I

### Connection Planning

- System Network Approval Process (SNAP) identification number
- Obtain cloud IPs
- Cloud Permission to Connect (CPTC)
- Obtain Cybersecurity Service Provider (CSSP)
- Contract vehicle
- Approved commercial provider account

## Phase II

### Connection Request

- System Network Approval Process (SNAP) registration (4 days after submission)
- Request SCCA services
  - SNAP ID
  - Application data (IPs/subnets)
  - CPTC
  - Technical exchange (as required)

## Phase III

### Connection & Sustainment

- Connection and validation testing
- CSSP feeds connected
- Application owner customizes environments to meet mission requirements

**SNAP Required Artifacts**

- Authorization Decision Document (ADD)
- Security Assessment Report (SAR)
- Security Plan (SP)
- Plan of Action and Milestones (POA&M)
- Detailed Topology Diagram
- Consent to Monitor (CTM)

# Onboarding and Ordering Information

- **Onboarding portal:**
  - **https://disa.deps.mil/ORG/SD/SD8/SCCA/MissionPartners/SitePages/Secure%20Cloud%20Computing%20Architecture.aspx**
- **DISA cloud portfolio:**
  - **https://www.disa.mil/Computing/Cloud-Services**

# visit us

DISA Booth 1929

# follow us

Facebook/USDISA

Twitter/USDISA

# meet with us

Industry partners can request a meeting with DISA by completing a form at **www.disa.mil/about/industry-partners**.

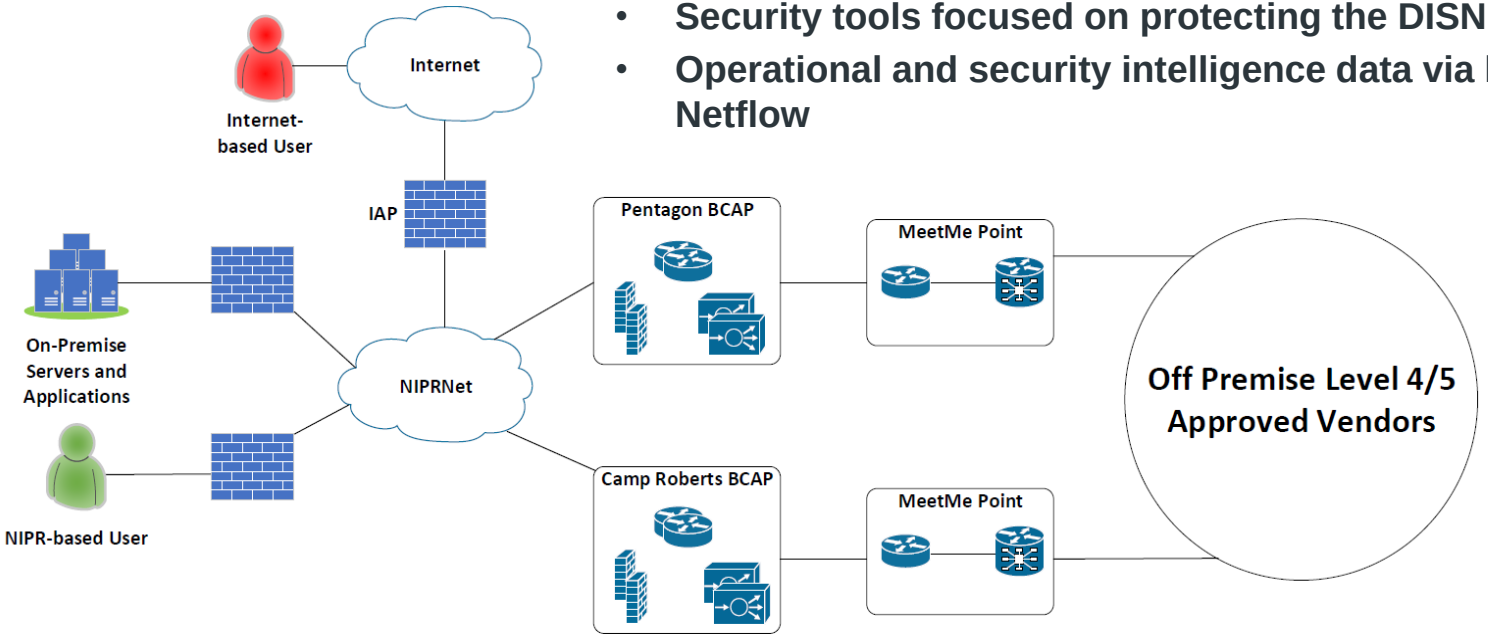

**DEFENSE INFORMATION SYSTEMS AGENCY**
The IT Combat Support Agency

**www.disa.mil** **/USDISA** **@USDISA**

# Boundary CAP (BCAP) 1.0 Overview

## Key Features

- NIPRnet connectivity support for IaaS and SaaS clouds
- Security tools focused on protecting the DISN from the cloud
- Operational and security intelligence data via logging and Netflow



# VDSS and VDMS 1.0 Overview

## VDSS Key Features

- Traditional DMZ security features for public facing web applications
- Next Generation Firewall for protecting cloud hosted workloads

## VDMS Key Features

- Cloud connected management and security tools
- Cloud privileged user access and account management
- Central search and display of CAP and cloud logs